

REMARKS/ARGUMENTS

Reconsideration and allowance of this application are respectfully requested. Currently, claims 1, 4-16, 21-26 and 29-31 are pending in this application.

Request for Approval of Replacement Drawing

Applicant filed a replacement sheet of drawings for Fig. 2 and an Annotated Sheet Showing Changes with the Amendment/Response filed March 22, 2004. Applicant respectfully requests entry and approval thereof.

Rejection Under 35 U.S.C. §102:

Claims 1, 4-16, 21-26 and 29-31 were rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Thatcher et al (U.S. '067, hereinafter "Thatcher"). Applicant respectfully traverses this rejection .

For a reference to anticipate a claim, each element must be found, either expressly or under principles of inherency, in the reference. Applicant submits that Thatcher fails to disclose each element of the claimed invention. For example, Thatcher fails to disclose "at the secure module of the or each selected user, in response to the said control message, controlling the availability of keys generated from the seed value, thereby controlling access by the users to the said data," as required by independent claim 1 and its dependents. Similarly, Thatcher fails to disclose "in response to the said control message, controlling the availability of keys generated using the said seed value and thereby controlling

access by the user of the customer terminal to data received at the customer terminal,” as required by independent claim 11 and its dependents. Thatcher also fails to disclose “control means arranged to only release keys for decrypting those respective frames for which a control field is received, and being arranged to, in response to the said control messages in the control fields, control the availability to the users of keys generated from the seed value,” as required by independent claim 12 and its dependents.

As an exemplary claim, claim 1 requires that a seed value for key generation is communicated to a secure module of a user. The secure module then generates keys from the seed value. The availability of the generated keys are controlled in response to control messages sent with data frames. The keys are used to decode the data frames. In such an arrangement, providing the secure module with the seed value has thus given it the ability to decode the received data frames. The control message which will determine whether or not the secure module performs decoding are sent (e.g., at a later time) with the data frames.

Thatcher discloses a cable head-end operator (i.e., not subscribers of the cable-end operator) implementing an encryption control system 110. The encryption control system 110 essentially forms a gateway that transforms a national entitlement management message (a national EMM) extracted from a global/national cable-tv data stream for the local use of a cable head-end user (a local distributor). Encryption control system 110 includes a first secure

microprocessor 120 for decrypting in decryptor 124 the national EMMs that have been encrypted with a global/national distribution key. The encryption control system 110 also includes a second secure microprocessor 130 for re-encrypting in encryptor 134 the EMM with a local key. Thatcher thus merely discloses a cable head-end operator (a local distributor) implementing a control system for decrypting EMMs that have been encrypted with a global/national key and re-encrypting them with a local key. (See, e.g., col. 5, line 56 to col. 6, line 38 of Thatcher).

The teachings of Thatcher therefore bear little relevance to the present invention. For example, Thatcher fails to disclose controlling the availability of keys generated from a seed value in response to a control message of a control field that has been distributed with a data frame. The Office Action apparently alleges that col. 6, lines 56-67 of Thatcher teaches this feature. Applicant respectfully disagrees. Col. 6, lines 56-67 states the following:

“In FIG. 7, encryption control system 140 includes de-multiplexer 112, multiplexer 114, first secure microprocessor 120 and second secure microprocessor 130. First secure microprocessor 120 includes secret serial number memory 122, decryptor 124 and multi-service key memory 126 performing substantially the same function as is performed in secure microprocessor 120 of encryption control system 110 (FIG. 6). Secure microprocessor 120 of encryption control system 140 (FIG. 7) also includes decryptor 142 to process the national entitlement control message using the multi-session key to recover seed data and service authorization data.”

No portion of the above passage describes controlling the ability of keys generated from a seed value in response to control message of a control field distributed with a data frame. This portion of Thatcher merely describes an encryption control system 140 of a cable head-end operator (a local distributor, rather than an end-subscriber of the cable head-end operator) for decrypting a national EMM and re-encrypting the message into a local EMM using a local key. As noted above, this bears little resemblance to the claimed invention.

Col. 4, lines 52-58 of Thatcher indicates that “Entitlement management messages are sent infrequently, for example, once per month....” It is therefore difficult to even begin considering how the decryption and local re-encryption of the infrequently sent EMMs in Thatcher discloses controlling the availability of keys generated from a seed value in response to control message of a control field distributed with a data frame. Applicant therefore respectfully requests that the next Office Action provide clarification if the rejection over Thatcher is maintained.

While encryption control system 110 provides multi-session keys to decoders, there is no teaching or even suggestion of controlling the availability of these keys to thereby control access by the users to data in response to a control message in a control field distributed with a data frame. None of col. 4, lines 38-46, col. 5, lines 13-24 and col. 5, lines 29-37 (each specifically identified by the Office Action) discloses this feature.

FAIRMAN et al.
Application No. 09/555,929
November 8, 2004

Accordingly, Applicant submits that claims 1, 4-16, 21-26 and 29-31 are not anticipated by Thatcher and respectfully requests that the rejection of these claims under 35 U.S.C. §102 be withdrawn.

Conclusion:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Raymond Y. Mah
Reg. No. 41,426

RYM:sl
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4044
Facsimile: (703) 816-4100